

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): John E. Cavanaugh, Roy M. Brooks, and Paul M. Quinn
Serial No.: 10/620,981
For: METHODS AND APPARATUS FOR NETWORK MESSAGE TRAFFIC
REDIRECTION
Filing Date: July 16, 2003
Examiner: Baotran N. To
Art Unit: 2135
Conf. No.: 8822

Certificate of Transmission Under 37 C.F.R. §1.8

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office via the EFS-Web system on:

Date: July 19, 2007

By: Farah Zafar
(Typed or printed name of person mailing
Document, whose signature appears below)

Signature: /FZ/

MAIL STOP AF

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313

Sir:

AMENDMENT

In response to the Office Action mailed on April 19, 2007, please amend the above-identified Application as follows:

-2-

IN THE CLAIMS

What is claimed is:

1. (Currently Amended) A method for redirecting network message traffic comprising
receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;
rerouting all message traffic carried via the first transport mechanism in the communications network, and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic,
rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex; and
directing the filtering complex to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node, directing the filter complex further comprising propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism.
2. (Previously Presented) The method of claim 1 further comprising directing the filter complex to filter the message traffic to subdivide desirable message traffic from undesirable message traffic.
3. (Original) The method of claim 1 wherein the filter complex further comprises a security filter having filtering logic for performing filtering, the security filter operable to parse the message traffic and identify sequences in the message traffic indicative of undesirable message traffic.

4. (Original) The method of claim 3 wherein the filter complex further includes a filter routing device in communication with other routing devices in the communications network and coupled to the security filter for analyzing message traffic.
5. (Original) The method of claim 4 wherein the filter routing device in the filtering complex is operable to communicate according to the first transport mechanism and the second transport mechanism.
6. Canceled
7. (Original) The method of claim 1 wherein directing further comprises directing a target node router serving the target node from the network management server, the network management server operable to send a redirect message to the target node router.
8. (Original) The method of claim 6 wherein the reroute message is indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via the target node router serving the target node.
9. (Original) The method of claim 7 wherein the redirect message is indicative that the target router serving the target node is not to receive message traffic according to the first transport mechanism corresponding to the target node.
10. (Original) The method of claim 7 wherein the redirect message is indicative that the target node router serving the target node receives the desirable message traffic in the second transport mechanism corresponding to the target node.
11. (Original) The method of claim 1 wherein first and second transport mechanisms coexist on a common physical network.

12. (Original) The method of claim 1 wherein first transport mechanism corresponds to a public access protocol adapted for communication via a plurality of dissimilar network switching devices.

13. (Original) The method of claim 1 wherein the second transport mechanism corresponds to a virtual private network operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network.

Claims 14-15. Canceled

16. (Original) The method of claim 1 wherein rerouting all message traffic is a static route, according to the first transport mechanism, from a single router serving the target node to the filter router serving the filter complex.

17. (Previously Presented) The method of claim 1 wherein receiving an indication further comprises detecting a recognizable pattern of inundating undesirable message traffic.

18. (Original) The method of claim 1 wherein the undesirable message traffic emanates from a plurality of sources, each of the plurality of sources independently contributing substantially insignificant volume of message traffic.

19. (Currently Amended) A network management server for redirecting undesirable message traffic comprising:

a network intrusion detector monitor operable to receive an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

a routing processor operable to propagate routing information from a routing table database to reroute all message traffic using the first transport mechanism directed to the particular target node; and

a connection to a filter complex responsive to the routing processor, the filter complex operable to distinguish desirable message traffic from undesirable message traffic, and further operable to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node, the filter complex operable to reroute all message traffic including propagating, via a standard protocol corresponding to the first transport mechanism, a node address other than the node address corresponding to the target node, the routing processor operable to direct the filter complex to propagate routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism, the network management server further operable to send a reroute message to the filter complex, in response to which the filter complex is operable to reroute the message traffic, the reroute message indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node.

20. (Previously Presented) The network management server of claim 19 wherein the filter complex is further operable to filter the message traffic to subdivide the desirable message traffic from the undesirable message traffic.

21. (Original) The network management server of claim 19 wherein the filter complex further comprises a security filter having filtering logic for performing filtering, the security filter operable to parse the message traffic and identify sequences in the message traffic indicative of undesirable message traffic.

22. (Original) The network management server of claim 21 wherein the filter complex further includes a filter routing device in communication with other routing

devices in the communications network and coupled to the security filter to analyze message traffic.

23. (Previously Presented) The network management server of claim 22 wherein the filter routing device in the filtering complex is operable to communicate according to the first transport mechanism and the second transport mechanism.

24. Canceled

25. (Original) The network management server of claim 19 wherein the routing processor is further operable to direct a target node router serving the target node from the network management server, the network management server operable to send a redirect message to the target node router.

26. Canceled

27. (Original) The network management server claim 25 wherein the routing processor is further operable to send a redirect message indicative that the target router serving the target node is not to receive message traffic according to the first transport mechanism corresponding to the target node.

28. (Original) The network management server claim 25 wherein the redirect message from the routing processor is further indicative that the target node router serving the target node receives the desirable message traffic in the second transport mechanism corresponding to the target node.

29. (Original) The network management server of claim 19 wherein a network interface in the network management server is compatible with the first and second transport mechanisms and wherein first and second transport mechanisms coexist on a common physical network.

30. (Original) The network management server of claim 19 wherein first transport mechanism is operable according to a public access protocol adapted for communication via a plurality of dissimilar network switching devices.

31. (Original) The network management server of claim 19 wherein the second transport mechanism is operable according to a virtual private network protocol operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network.

32. (Original) The network management server of claim 19 wherein the filter complex is operable to reroute all message traffic including propagating, via a standard protocol corresponding to the first transport mechanism, a node address other than the node address corresponding to the target node.

33. (Original) The network management server of claim 19 wherein the routing processor is operable to direct the filter complex to propagate routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism.

34. (Previously Presented) The network management server of claim 19 wherein the routing processor is operable to rerouting the message traffic according to a static route in the first transport mechanism, from a single router serving the target node to the filter router serving the filter complex.

35. (Original) The network management server of claim 19 wherein the undesirable message traffic emanates from a plurality of sources, each of the plurality of sources independently contributing substantially insignificant volume of message traffic.

36. (Currently Amended) In a network management server of a networked system of data communications devices, a method for transparently intercepting, filtering, and rerouting message traffic for recovering from a distributed denial of service attack comprising:

detecting, at a network monitor in the network management server, a pattern of inundating undesirable message traffic to a particular target node transported via a first transport mechanism in a communications network;

receiving, via a routing processor, an indication of the undesirable message traffic directed to the particular target node;

transmitting, via a network interface, a reroute message to a filter complex having a security filter operable to distinguish desirable message traffic from undesirable message traffic; and

rerouting, via a filter routing device in the filter complex, all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex, the reroute message indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node;

filtering, at the security filter, the message traffic to bifurcate desirable message traffic from undesirable message traffic;

transmitting, via the network interface to a target node router serving the target node, a redirect message indicating that the target node router is to receive, via the second transport mechanism, the desirable message traffic directed to the particular target node and rerouted to the filter complex, the filter complex and the target node router conversant in the first transport mechanism and the second transport mechanism; and

directing, from the network management server, the filtering complex to transmit, via a second transport mechanism over the communications network, the desirable

message traffic to the target node, directing the filter complex further comprising propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism.

37. (Currently Amended) A computer program product having an encoded set of processor based instructions on a computer readable medium operable to store computer program logic embodied in computer program code encoded thereon for directing a processor to perform steps for redirecting network message traffic comprising:

- computer program code for receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

- computer program code for rerouting all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic, rerouting all message traffic further comprising propagating, via a standard protocol corresponding to the first transport mechanism, a node address other than the node address corresponding to the target node, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex, the reroute message indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node; and

- computer program code for directing the filtering complex to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node, the first transport mechanism and the second transport mechanism having different sets of routing tables, directing the filter complex further comprising propagating routing information according to a predetermined protocol, the

routing information operable to designate the target node as the destination of the message according to the second transport mechanism.

38. (Currently Amended) An encoded set of processor based instructions tangible encoded on a computer readable medium embodying program code for redirecting network message traffic comprising:

program code for receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

program code for rerouting all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex, the reroute message indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node; and

program code for directing the filtering complex to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node, the second transport mechanism corresponding to a virtual private network operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network, means for directing the filter complex further comprises:

means for propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism.

39. (Currently Amended) A network management server for redirecting undesirable message traffic comprising:

-11-

means for receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

means for rerouting all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic, rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex, the reroute message indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via a target node router serving the target node; and

means for directing the filtering complex to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node, the second transport mechanism corresponds to a virtual private network operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network.

-12-

REMARKS

In response to the Office Action mailed on April 19, 2007, Applicants respectfully request reconsideration. Claims 1-13 and 16-39 are now pending in this Application. Claims 1, 19 and 36-39 are independent claims and the remaining claims are dependent claims. In this Amendment, claims 1, 19 and 36-39 have been amended and claims 6, 24 and 26 have been canceled. Applicants believe that the claims as presented are in condition for allowance. A notice to this affect is respectfully requested.

Preliminary Matters:

The Office Action finally rejects claims 1-13 and 16-39 based on Ylonen '379, a new ground of rejection. Amended claim 1, however, was amended with dependent Claim 14, and thus the scope of amended claim 1 is exactly the same as originally filed claim 14, to recite propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism, as clarified in the response of the previous office action filed January 16, 2007. Applicant submits that it is improper to finally reject this original claim upon the first citation of a new reference. Therefore, applicant respectfully requests that the finality of the Office Action be withdrawn and the response herein considered accordingly.

Claim(s) 1-13 and 16-39 have been rejected under **35 U.S.C. §103(a)** as being obvious over Afek, U.S. Pub. No. 2002/0083175 (hereinafter Afek '175) in view of Ylonen, U.S. Pub. No. 2003/0110379 (hereinafter Ylonen '379). With respect to the new rejections at hand, Ylonen '379 does not show a reroute message for rerouting in an overlay manner, as discussed further at page 5, lines 5-13. Rather, Ylonen '379 takes one of two distinct paths based on routing considerations (paragraph [0039] and source A and source B in the cited example), not on overlay path between the same endpoints.

The claimed reroute message approach differs from the Ylonen '379 approach because the reroute exhibits an overlay arrangement, not a separate path as in Ylonen

(Sources A and B of Figs. 2a-2c) The claimed second path adheres to the second protocol. Which in the example shown corresponds to a VPN, to transport the message traffic between the same source and destination via an overlay path. Accordingly, Claim 1 has been amended with the subject matter of claim 6, to clarify that rerouting all message traffic including directing the filter complex from a network management server in communication with the filter complex, the network management server operable to send a reroute message to the filter complex.

While the Office Action suggests that Claim 6 is anticipated by paragraphs [0286] and [0298] of Afek, as the Office Action concedes, Afek '175 does not show rerouting according to the second transport mechanism, as amended in the response to the previous office action (response of Jan. 16, 2007). Claim 19, rejected on similar grounds, has been similarly amended with subject matter of claim 24, and has been further amended with the subject matter of claim 26, to clarify the distinguishing features of the reroute message by reciting that the reroute message [is] indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via the target node router serving the target node. As claim 26 previously depended from claims 24 and 19, it is further submitted that no new search considerations are raised by this amendment. Claims 36-39, also rejected on similar grounds, have been similarly amended.

Further, one of skill in the art would seek to achieve the present invention by modifying Afex '175 according to Ylonen '379 because Afek '175 is concerned with recovery processing following a DDOS (Distributed Denial of Service) attack. Such a DDOS attack inundates a server with excessive unintended and/or malicious message traffic that inhibits performance at the inundated server. The cited Ylonen '379 reference addresses defensive operations in maintaining an application to prevent undesirable message traffic. In preventing a DDOS attack, the message quantity, not content, is of concern, while Ylonen '379 is concerned with interrogating message content to proactively flag an undesirable payload. [0009], [0015]. In other words, a Ylonen '379 approach guards against message content, while the claimed approach

-14-

solves the problem of undesirable message volume. It is therefore respectfully submitted that Ylonen '379 does not show, teach or disclose, alone or in combination with Afek, the claimed invention as recited in claim 1, and in further amended independent claims 19 and 36-29.

As the remaining claims depend, either directly or indirectly, from claims 1 and 19, it is respectfully submitted that all claims in the case are now in condition for allowance.

Applicant(s) hereby petition(s) for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-9660, in Westborough, Massachusetts.

Respectfully submitted,

/CJL/

Christopher J. Lutz, Esq.
Attorney for Applicant(s)
Registration No.: 44,883
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: CIS03-25(7365)

Dated: July 19, 2007